II. IN THE SPECIFICATION

Please replace the Abstract of The Invention with the following:

A system and method for consistent authentication and security mechanism to enable a client device to easily roam from one network to another without requiring the client to manually change network configurations is disclosed. In one embodiment, a client device listens for a "beacon frame" broadcast from a Wi-Fi access point. The beacon frame identifies the basic service set identifier (BSSID) of the access point. A tamper-resistant token, or client key, installed at the client device stores a set of authentication parameters, e.g., cryptographic keys, for each Wi-Fi network the client is permitted to access. Each set of authentication parameters is associated with a particular BSSID. Using the BSSID received from the access point, the client device identifies and implements the appropriate set of authentication parameters necessary to authenticate the client device according to an authentication process generally accepted by all the Wi-Fi networks potentially servicing the client.

Please amend paragraph [0001] as follows:

[0001] This present application claims priority to U.S. Provisional Patent Application No. 60/416,583 filed on Oct. 8, 2002; U.S. Provisional Patent Application No. 60/422,474 filed Oct. 31, 2002; and U.S. Provisional Patent Application No. ~~60/447,921~~ **60/477,921** filed Jun. 13, 2003. The contents of these three provisionals are incorporated herein by reference in their entirety. The present application is related to U.S. Patent Application No. ~~10/xxx,xxx~~ **10/679,472**, entitled "Self-Managed Network Access Using Localized Access Management," and U.S. Patent Application No. ~~10/xxx,xxx~~ **10/679,371** entitled "Localized Network Authentication and Security Using Tamper-Resistant Keys," both of which are filed concurrently herewith.

Please amend paragraph [0010] as follows:

[0010] As the user moves from network to network, for instance from his office network to a public network at a coffee shop, the user must switch his Wi-Fi setting as appropriate for the local network. Generally, this requires advanced knowledge of the settings for the new network. ~~Microsoft Windows~~ MICROSOFT WINDOWS® operating systems facilitate the storage of these settings as a "location," thereby enabling the user to simply point-and-click to select the new network. However, the user still must manually install these parameters for the new network during initial setup.

Please amend paragraph [0012] as follows:

[0012] Of further difficulty for a host facility of a Wi-Fi network such as an airport, generally there can only be one Wi-Fi network hosted per location. For example, Wi-Fi networks are shared-used networks. That is, Wi-Fi networks are unlicensed and hence there is no protection against interference from an additional network being installed at the same location. Once the first network is installed, say a ~~Wayport~~ WAYPORT®. network, which provides travelers with wireless Internet access, no other network can be installed without interference resulting from the second network. The host facility generally prefers that all potential customers have access to the wireless network, not just ~~Wayport~~ WAYPORT customers. However, a ~~Wayport~~ WAYPORT network only admits ~~Wayport~~ WAYPORT customers. Therefore, the issue becomes how do you allow a private network to admit customers from other networks to utilize the private network.

Please amend paragraph [0013] as follows:

[0013] Companies like ~~Boingo~~ BOINGO™. offer a service whereby users can roam across multiple networks without necessarily being a customer of any particular network. ~~Boingo~~ BOINGO employs a ‘sniffer’ program which listens to the beacon frames and looks for a match in it's database of known network configurations. When a match is found, the ~~Boingo~~ BOINGO software will automatically make the appropriate configuration changes for that network and allow the user to connect. Once connection is attempted, the user appears to the network as a ~~Boingo~~ BOINGO customer and the user's credentials are passed onto an authentication server for the network. On recognition of the user's name at the authentication server, for example, access is then granted or denied. If the ~~Boingo~~ BOINGO customer is not really a customer of the present network, the authentication server forwards the user's credentials to a ~~Boingo~~

BOINGO authentication server, which performs the authentication service and if valid, passes the 'grant' command back to the original network authentication server. One problem with this approach is that as the number of 'network affiliates' grows for ~~Boingo~~ **BOINGO**, each network's configuration must be stored in a database. Accordingly, information in this database must be downloaded to each user. This becomes difficult to manage as the number of users and networks increase.

Please amend paragraph [0041] as follows:
[0041] The master key 230, client keys 240A-N, and AP key 250 overlap in functionality. Particularly, each physical key comprises an embedded tamper-resistant subscriber identity module (SIM) token 232, 242A-N, or 252, respectively, unique to each key. In an embodiment of the invention, a ~~Cryptoflex~~ **CRYPTOFLEX™** USB-enabled SIM chip is employed as the SIM token. Nevertheless, other conventional or foreseeable SIMs may be substituted. The AP key 250 differs slightly from both the master key 230 and the client keys 240A-N in that it preferably employs a device USB connector rather than a standard USB connector. Generally, a device USB connector is different from a standard USB connector only in physical layout. Yet, they each carry the same signal wires to provide a USB interface to the USB-enabled SIM chip, which typically communicates over a simplex data line at approximately 9600 bits-per-second. Importantly, each physical key has a unique serial number stored permanently and electronically inside the SIM by the manufacturer to provide positive identification. Each SIM comprises a random number generator.